DATE(S) ISSUED:
08/09/2011

SUBJECT:
Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (MS11-060)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Visio, a program used forcreating flowcharts and diagrams. These vulnerabilities can be exploited by opening a specially crafted Visio file (.VSD) received as an email attachment, or by visiting a website and opening a specially crafted Visio file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
·   Microsoft Visio 2003
·   Microsoft Visio 2007
·   Microsoft Visio 2010

RISK:
Government:
·   Large and medium government entities: **High**
·   Small government entities: **High**

Businesses:
·   Large and medium business entities: **High**
·   Small business entities: **High**

Home users: Low - due to our assumption that Visio is not widely utilized by an average home user

DESCRIPTION:
Two new vulnerabilities have been identified in Microsoft Visio that could allow remote code execution. These remote code execution vulnerabilities are due to the way that Microsoft Visio validatesobjects in memory or parses certain structures when handling a specially crafted Visio file (.VSD). These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Visio file as an email attachment. In the Webbased scenario, a user would visit a website and then open the specially crafted Visio file that is hosted on the page.

RECOMMENDATIONS:
The following actions should be taken:
·   Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
·   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
·   Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

·   Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

·   Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/ms11-060.mspx

SecurityFocus:
http://www.securityfocus.com/bid/49021
http://www.securityfocus.com/bid/49024

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1972
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1979